In the claims:

1. (currently amended) Method for preserving security associations between at least two member entities of a secure group comprising the steps of:

maintaining a security association relating to communication between the at least two member entities in volatile storage of a key server operative to distribute security associations;

storing a copy of the security association in non-volatile storage associated with the key server; and

in response to detection of corruption of the security association in volatile storage, where the corruption is caused by an event other than power failure, employing the copy of the security association in non-volatile storage to update the security association in volatile storage.

2. (previously presented) The method according to claim 1, further comprising the step of encrypting the security association prior to storing the security association in the non-volatile storage.

3. (previously presented) The method according to claim 1 wherein the step of storing includes the step of detecting a trigger event.

4. (previously presented) The method according to claim 3 wherein the step of detecting a trigger event includes the step of detecting a change in the security association.

5. (previously presented) The method according to claim 1 further comprising the step of updating the contents of a security associations table using the security association stored in non-volatile storage.

6. (cancelled)

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (currently amended) An apparatus for distributing and preserving security associations between at least two member entities of a secure group comprises:

a volatile memory including a first table for storing a security association related to communication between the at least two entities;

a non-volatile memory including a second table for storing at least a portion of the first table;

means for copying the at least a portion of the first table to the second table; and

means for copying at least a portion of the second table to the first table in response to detection of corruption of the first table, where the corruption is caused by an event other than power failure.

11. (previously presented) The apparatus of claim 10, further comprising means for encrypting the at least a portion of the first table prior to copying the at least a portion of the first table to the second table.

12. (previously presented) The apparatus of claim 10 further comprising means for copying overwriting the at least a portion of the first table with contents of the second table.

13. (previously presented) The apparatus of claim 10 including encryption logic for encrypting the at least a portion of the first table.

14. (previously presented) The apparatus of claim 10 including decryption logic for decrypting the second table.

15. (previously presented) The apparatus of claim 10 further comprising a key, stored in non-volatile memory, for encrypting the at least a portion of the first table.